



विषय:- साइबर घटना अथवा संकट हेतु तैयारी के संबंध में
Sub: - Regarding Cyber Incident or Crisis Preparedness

प्रति / To,

सभी विनियमित संस्थाएँ, आईआईबी और प्रशिक्षण संस्थान
All Regulated Entities, IIB and Training Institutes

1. आज के डिजिटल युग में कोई भी साइबर घटना और / या संकट संस्थाओं के लिए महत्वपूर्ण आशंकाएँ उत्पन्न करता है और इसलिए ग्राहक डेटा सहित सूचना आस्तियों के लिए किसी भी क्षति को रोकने या उसे न्यूनतम करने तथा व्यवसाय की निरंतरता सुनिश्चित करने के लिए प्रभावी ढंग से प्रतिक्रिया दर्शाने के लिए तैयार रहना निर्णायक होता है।

2. इस संबंध में, शीर्षकित विषय के संबंध में आईआरडीएआई सूचना और साइबर सुरक्षा दिशानिर्देश, 2023 के विभिन्न उपबंधों की ओर ध्यान आकर्षित किया जाता है:

क) पालिसी सं. 2.10 के अंतर्गत पैरा 3.5 तथा आईआरडीएआई परिपत्र संदर्भ: आईआरडीएआई/जीए&एचआर/सीआईआर/विविध/128/06/2023 दिनांक 13. 06. 2023 अर्थात् विनियमित संस्थाएँ (आरईएस) ऐसी घटनाओं के बारे में **किन्हीं साइबर घटनाओं की सूचना उसका पता लगने या जानकारी में लाये जाने से 6 घंटे के अंदर निर्धारित फॉर्मेट में आईआरडीएआई को दें।**

ख) पालिसी सं. 2.16 के अंतर्गत पैरा 3.3 अर्थात् निगरानी, लॉगिंग और निर्धारण पैरा:

- I. सभी आईसीटी अवसंरचना और अनुप्रयोग लागों का **अनुरक्षण और निगरानी 180 दिन की निरंतर अवधि के लिए** की जाए;
- II. संस्था अथवा सुरक्षा क्षेत्र के अंदर सभी संगत सूचना प्रसंस्करण प्रणालियों की घड़ियाँ राष्ट्रीय सूचना-विज्ञान केन्द्र (एनआईसी) अथवा राष्ट्रीय भौतिक प्रयोगशाला (एनपीएल) अथवा एनटीपी सर्वरों के साथ इन एनटीपी सर्वरों के लिए खोज के लायक नेटवर्क समय प्रोटोकाल (एनटीपी) के साथ समकालिक कर दी जाएँगी।

ग) पालिसी सं. 2.18 के अंतर्गत पैरा 3.3 अर्थात् परिस्थितिगत जागरूकता साइबर आक्रमणों के लिए संस्थाओं की प्रतिक्रिया के भाग के रूप में **साइबर संकट प्रबंध योजना (सीसीएमपी)** हेतु व्यवस्था करती है;

घ) पालिसी सं. 2.20 के अंतर्गत पैरा 3.4 अर्थात् साइबर आघात-सहनीयता, तीव्र सूचना सुरक्षा घटनाओं के लिए **न्यायिक जाँच निष्पादित करने** हेतु व्यवस्था करती है। सीआईएसओ का



एक कार्य भी ऐसे न्यायिक विशेषज्ञों की संबद्धता के लिए व्यवस्था करता है जो प्रमाणित हैं एवं आवश्यकता होने पर इस कार्य के लिए सक्षम हैं।

उ) सामान्य दिशानिर्देशों के अंतर्गत पैरा 1.10 ने व्यवस्था की है कि विनियमित संस्थाएँ समय-समय पर सर्ट-इन द्वारा जारी किये गये निदेशों का पालन करेंगी जिनमें सूचना सुरक्षा प्रथाओं, प्रक्रिया, निवारण, प्रतिक्रिया तथा सुरक्षित और विश्वसनीय इंटरनेट के लिए साइबर घटनाओं की रिपोर्टिंग के संबंध में सर्ट-इन निदेश दिनांक 28 अप्रैल 2022 के अनुसार सर्ट-इन को घटना की रिपोर्टिंग से संबंधित निदेश भी शामिल है।

3. यह पुनः एक बार दोहराया जाता है कि सभी विनियमित संस्थाएँ प्रभावी तैयारी को सुनिश्चित करने के लिए साइबर घटना/संकट के लिए तैयारी संबंधी उपर्युक्त उपबंधों का **अवश्य कड़ाई से पालन करें।**

4. उपर्युक्त के अतिरिक्त, सभी विनियमित संस्थाओं से अपेक्षित है कि वे **यह सुनिश्चित करने के लिए एक सुपरिभाषित प्रक्रिया / प्रथा स्थापित करें कि न्यायिक संपरीक्षक पहले से ही सूचीबद्ध हों तथा उन्हें अविलंब साइबर घटना/ओं की न्यायिक जाँच संचालित करने और उनका मूल कारण विश्लेषण करने के लिए संबद्ध किया जा सके।**

5. इसके अलावा, यह अवश्य सुनिश्चित किया जाना चाहिए कि सुरक्षा परिचालन केन्द्र (एसओसी), आक्रमण तल निगरानी, रेड टीमिंग, अथवा वार्षिक आश्वासन संपरीक्षण अथवा विनियमित संस्था के किसी भी साइबर सुरक्षा पहलू को संभालनेवाले विक्रेता को घटना के लिए न्यायिक संपरीक्षक के रूप में संबद्ध न किया जाए जिससे **हितों के संघर्ष का निवारण किया जा सके।**

6. बीमा मध्यवर्तियों सहित, सभी विनियमित संस्थाओं को सूचित किया जाता है कि वे बोर्ड की आगामी बैठक में उपर्युक्त उपबंधों का अनुपालन प्रस्तुत करें और बैठक का कार्यवृत्त सूचनार्थ प्राधिकरण को प्रस्तुत करें।

1. In today's digital age, any cyber incident and / or crisis pose significant threats to organizations and therefore it is crucial to be prepared to respond effectively to prevent or minimize damage to information assets, including customer data and ensure business continuity.

2. In this connection, attention is invited to various provisions of IRDAI Information and Cyber Security Guidelines, 2023, with respect to the captioned subject:

a) Para 3.5 under Policy no. 2.10 and IRDAI circular ref: Ref: IRDAI/GA&HR/CIR/MISC/128/06/2023 dated 13/06/2023 i.e. Regulated Entities (REs) to **report any cyber incidents to IRDAI in prescribed format within 6 hours of noticing or being brought to notice** about such incidents;

b) Para 3.3 under Policy no. 2.16 i.e. Monitoring, Logging and Assessment Para:



- I. all ICT infrastructure and application logs are to be **maintained and monitored for a rolling period of 180 days**;
- II. the clocks of all relevant information processing systems within Organization or security domain shall be synchronized with Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP Servers traceable to these NTP Servers.
 - c) Para 3.3 under Policy no. 2.18 i.e. Situational Awareness provides for **Cyber Crisis Management Plan (CCMP)** as a part of organisations response for cyber-attacks;
 - d) Para 3.4 under Policy no. 2.20 i.e. Cyber Resilience provides for **performing forensic investigation** for severe information security incidents. One of the functions of CISO also provides engagement of external forensic experts who are certified as well as competent for the job as and when required.
 - (e) Para 1.10 under General Guidelines provided that Regulated Entities shall adhere to directions issued by Cert-In from time to time including relating to Incident Reporting to the CERT-In as per CERT-In direction dated 28th April 2022 on information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
3. It is once again re-iterated that all Regulated Entities **must strictly adhere** to the above provisions on cyber incident/crisis preparedness to ensure effective readiness.
4. In addition to the above, all Regulated Entities are required to **establish a well-defined procedure / practice to ensure that the forensic auditor/s are empanelled in advance and can be onboarded to conduct** forensics and root cause analysis of cyber incident/s **without any delay**.
5. Furthermore, it must be ensured that the vendor handling Security Operation Centre (SOC), attack surface monitoring, Red teaming, or conducting the annual assurance audit or any cyber security aspect of Regulated Entity is not engaged as the forensic auditor for the incident to **avoid a conflict of interest**.
6. All Regulated Entities, including insurance intermediaries are advised to place compliance to the above provisions to their Board in the ensuing Board Meeting and submit the minutes of the meeting to the Authority for information.

(ए. आर. नित्यानंथम/ A. R. Nithiyanantham)
कार्यकारी निदेशक (सा.प्र.& मा.सं.)/ Executive Director (GA & HR)